IN THE CLAIMS

Please amend claims 1, 2, 4, 6-15, and 17 as follows:

1. (Currently Amended) A method of conducting a transaction between a first entity and a second entity where as part of the transaction the second entity ~~or an examination agent operating on behalf of the second entity~~ requires information to assess a level of risk associated with transacting with the first entity, the method comprising ~~the steps of~~:

~~a)~~ a first data processor acting on behalf of the first entity requesting a second data processor acting on behalf of the second entity to provide trust data about ~~itself~~ a trust level of the second data processor;

~~b)~~ the first data processor acting on behalf of the first entity ~~analysing~~ analyzing the trust data ~~response~~ and determining an assessment of trust of the second data processor operating on behalf of the second entity;

~~c)~~ defining a pseudonymous identity for the first entity; **[[ ]]**and

~~d)~~ providing real data about the first entity to the second entity where the real data is selectively ~~withheld or generalised~~ generalized into mapped data in response to the assessment of trust.

2. (Currently Amended) A method of conducting a transaction as claimed in claim 1, in which the method further comprises ~~the step of~~ entering into a contract for the transaction based on the mapped data provided about the first entity such that the identity of the first entity remains unknown to the second entity.

3. (Original) A method as claimed in claim 1, in which the transaction is the purchase of insurance, and for a given type of insurance the pseudonymous identity is associated with sufficient information to enable the insurer or an insurance examination agent to assess a level of risk for pricing or issuing an insurance.

4. (Currently Amended) A method as claimed in claim 3, in which, when seeking to claim on the insurance policy, the real data and a true identity pertaining to the first entity

are made available to the insurer in order that the insurer can validate that there is an acceptable level of correlation between the pseudonymous identity and the first entity.

5. (Original) A method as claimed in claim 1, in which the first entity submits their information or responses via a trusted computer, and wherein a trusted platform module within the trusted computer generates a user identity which can be used in future to confirm the identity of the first entity.

6. (Currently Amended) A method as claimed in claim 1, in which the first entity enters ~~their~~ the real data onto a trusted computer together with their policy agent which defines how information relating to the first entity can be disclosed.

7. (Currently Amended) A method as claimed in claim 4, in which the transaction relates to the purchase of insurance and the policy agent communicates with an insurance examination agent in order to negotiate and ~~authorise~~ authorize an insurance policy.

8. (Currently Amended) A method as claimed in claim 5, in which the transaction relates to the purchase of insurance and the trusted computing platform module and a server running the examination agent authenticate with one another such that the policy issued to the first entity via the pseudonymous identity is linked to an identity used in the authentication or to a further identifier provided by the first entity.

9. (Currently Amended) A method as claimed in claim 1, in which the ~~generalised~~ generalized data is generated by a ~~generalising~~ generalizing agent acting in accordance with a user's security policy.

10. (Currently Amended) A method of purchasing insurance, comprising ~~the steps of~~:

~~i)~~ an insurer making its conditions for insurance available to a third party;

~~ii)~~ a customer making ~~its~~ responses to ~~the conditions for~~ insurance questions available to the third party, ~~and~~

~~iii)~~ the third party ~~analysing~~ analyzing the responses and determining whether insurance can be offered to the customer based on the conditions for insurance, and if so validating to the insurer that a policy has been issued to the customer and that the customer satisfies the ~~insurer's~~ conditions for insurance, wherein

~~iv)~~ the customer enters ~~their~~ real data onto a trusted computer together with ~~their~~ a policy agent ~~which~~ that defines how information relating to the customer can be disclosed to an insurance examination agent, and the trusted computer interrogates ~~the~~ a data processing environment and policies of the third party to determine ~~how trustworthy~~ a trust level of the third party; ~~parties is, and selectively adjusts an amount of information which it discloses about the customer on the basis of the determination of trustworthiness~~

defining a pseudonymous identity for the first entity;

selectively generalizing the real data into mapped data in response to the trust level; and

providing the pseudonymous identity for the first entity and the mapped data to the insurance examining agent.

11. (Currently Amended) A method as claimed in claim 10, in which the transaction is conducted electronically and in which the customer submits ~~their~~ information or responses via a trusted computer, and wherein a trusted platform module within the trusted computer generates a user identity which can be used in future to confirm the identity of the customer.

12. (Currently Amended) A method as claimed in claim 10, in which, when seeking to claim on the insurance policy, the details of the first entity are made available to the insurer in order that the insurer can validate that there is an acceptable level of correlation between the ~~generalised~~ generalized identity and the first entity.

13. (Currently Amended) A method as claimed in claim 10, in which a pseudonymous identity is formed based on a ~~generalised~~ generalized identity, the pseudonymous identity including pseudonymous information which can be exchanged

with the insurer so that the insurer can validate that it is communicating with the first entity via its pseudonymous identity.

14. (Currently Amended) An apparatus for conducting a transaction comprising a first data processor acting on behalf of a first entity and a second data processor acting on behalf of a second entity, and where as part of the transaction the second entity or an examination agent operating on behalf of the second entity requires information to assess a level of risk associated with transacting with the first entity, wherein:

~~a)~~ the first data processor requests the second data processor to provide information about a trust level of the second data processor ~~itself~~ and ~~the~~ security policies of the second entity;

~~b)~~ the first data processor analyses the ~~response~~ the trust level and the security policies and assesses the amount of trust that should be attributed to the second data processor and/or the second entity;

~~c)~~ the first data processor defines a pseudonymous identity for the first entity;[[ ]] and

~~d)~~ the first data processor provides real information about the first entity to the second data processor where the real information is associated with the pseudonymous identity and where the real information ~~about the first entity~~ is selectively ~~withheld or generalised~~ generalized in response to the assessment of the amount of trust attributed to the second data processor and/or the second entity.

15. (Currently Amended) An apparatus as claimed in claim 14, in which the first computer executes a policy agent which controls how the real information relating to the first entity is disclosed.

16. (Original) An apparatus as claimed in claim 14, in which the first computer has a trusted platform module which generates a user identity which can be used to confirm the identity of the first entity.

17. (Currently Amended) The method of conducting a transaction between a first entity and a second entity according to claim 1 wherein the second entity comprises a selected one of a plurality of prospective second parties and wherein the first data processor acting on behalf of the first entity requests one or more data processors acting on behalf of each of the prospective second party to provide data about itself;

~~b)~~ the first data processor acting on behalf of the first entity ~~analysing~~ analyzing ~~the~~ responses and determining an assessment of trust of the data processor operating on behalf of each prospective second party;

~~c)~~ defining a pseudonymous identity for the first entity; and

~~d)~~ providing data about the first entity to a group of the prospective second parties where data is selectively ~~withheld or generalised~~ generalized for each prospective second party in said group of prospective second parties in response to the assessment of trust associated with each data processor operating on behalf each of said group of second parties.